

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:

INFORMATION ASSOCIATED WITH  
GOOGLE, LLC ACCOUNT  
GRANTKEPPEL@GMAIL.COM THAT IS  
STORED AT PREMISES CONTROLLED BY  
GOOGLE, LLC AT 1600 AMPHITHEATRE  
PARKWAY, MOUNTAIN VIEW, CA 94043

Mag. No. 20-414M

**Filed Under Seal**

INFORMATION ASSOCIATED WITH KIK  
ACCOUNT AND THE USERNAME  
“BLAIRALEX32” THAT IS STORED AT  
PREMISES CONTROLLED BY  
MEDIALAB.AI HEADQUARTERED AT  
1240 MORNINGSIDE WAY,  
VENICE, CA 90291

Mag. No. 20-415M

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR A SEARCH WARRANT**

I, Matthew Patcher, a Special Agent (SA) with the Federal Bureau of Investigation, being  
duly sworn, depose and state as follows:

**INTRODUCTION**

1. I make this affidavit in support of an application for a search warrant for information  
contained in or associated with (i) the Google, LLC electronic mail (email) account of  
**grantkeppel@gmail.com**, controlled by the web-based electronic communication service provider  
known as **Google, LLC**, headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043;  
and (ii) the **Kik** account associated with the username “**blairalex32**”, maintained and controlled by  
MediaLab.AI headquartered at 1240 Morningside Way, Venice, CA 90291, and accepting service of

legal process through email at lawenforcement@kik.com. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **Google, LLC** and **Kik (MediaLab.AI)** to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since October 2012. I am currently assigned to the Pittsburgh Division of the FBI, working Human Trafficking and Violent Crimes Against Children matters. Previously, I was assigned to the New York Division of the FBI where I was assigned to the Safe Streets Task Force, investigating street gangs and drug trafficking organizations. As such, I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and make arrests for offenses enumerated in Title 18, United States Code, Section 2510.

3. During my career in law enforcement, I have personally conducted and participated in numerous federal drug trafficking, human trafficking, and child exploitation investigations. I have been involved in narcotics and child exploitation related arrests and the execution of search warrants, and I have assisted in the supervision of activities of informants. Furthermore, I have participated in the investigation of numerous drug trafficking and human trafficking conspiracies, child exploitation

cases, and cases involving the use of court-authorized disclosure of location data relating to cellular telephones.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. I know that Title 18 U.S.C. Section 2251(a) makes it a crime to produce material depicting the sexual exploitation of a minor (child pornography); Section 2252(a)(1) criminalizes the knowing transportation of child pornography; Section 2252(a)(2) makes it a crime to knowingly receive or distribute material depicting the sexual exploitation of a minor, if the material was transported in or affecting interstate commerce by any means, including by computer; and Section 2252(a)(4)(B) makes it a crime to possess material depicting the sexual exploitation of a minor.

6. Through my experience and training, I am aware that Title 18, United States Code, Section 2256 defines “minor”, for purposes of Section 2252, as “any person under the age of eighteen years.” Section 2256 also defines “sexually explicit conduct” for purposes of these sections as including: (a) genital-genital, oral-genital, anal-genital, and oral-anal sexual intercourse, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251(a), 2252(a)(1), 2252(a)(2), and 2252(a)(4)(B) have been committed and are being committed by the

individual associated with the **Kik** username “**blairalex32**” associated with the **Google, LLC** email account **grantkeppel@gmail.com** (“Subject Accounts”). There is also probable cause to search for information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes, as particularly described in Attachment B.

### **JURISDICTION AND AUTHORITY TO ISSUE WARRANT**

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

9. Beginning in and around November 2019, the FBI identified an individual using the profile name “**blairalex32**” on the **Kik** messaging platform discussing child pornography. **blairalex32** entered a public chatroom named “Family Fun [family emoji][heart emoji]” where an FBI undercover agent was tracking conversations related to the sexual exploitation of minors. **blairalex32** sent two images of an 11-14 year old female, naked, standing in front of a mirror. **blairalex32** claimed the images were of his niece and offered to sell a link with more than 800 pictures. The FBI undercover sent a private message to **blairalex32**.

10. During the private message conversation, the undercover asked if **blairalex32** had videos as well. **blairalex32** responded he had 15 hours of Skype calls that depicted the same minor female. **blairalex32** again claimed the minor female was his niece. **blairalex32** said the link to the pictures would be \$50 and the video calls would be an additional \$50. The undercover asked for proof that **blairalex32** had access to sexually exploitive material. **blairalex32** sent a close-up video

of a female of unknown age, naked and rubbing a banana on her genitals. **blairalex32** sent a link to “CASHAPP” for transfer of funds. **blairalex32** said the female in the pictures and videos was twelve years old in the majority of the pictures and videos, but had turned thirteen years old in others.

11. Instead, the undercover offered to pay **blairalex32** via PayPal or some other method of payment. **blairalex32** agreed to PayPal but admonished the undercover not to share the PayPal account as it contained **blairalex32**’s real name. **blairalex32** said the e-mail associated with his PayPal is **grantkeppel@gmail.com**. The OCE sent **grantkeppel@gmail.com** \$50 via PayPal and in return received a link that contained hours of videos of the same minor female engaged in various sexual acts.

a. In one video, a recorded Skype session, a minor female approximately 11-13 years old is completely nude. The minor female is instructed to bend over and spread her legs making her vagina visible while an adult male on the other end of the call masturbates.

b. In another recorded Skype session, the same minor female is nude from the waist down. The minor female is asked, in sum and substance, if she would do anything to prevent videos of her being sent to others. She replies she would do anything to prevent the videos from being sent. The other party instructs the minor female to spread and rub her vagina. The minor female does as she is told.

12. After reviewing the material received from **blairalex32** your affiant was able to identify the female depicted as a victim in a different FBI investigation. The subject of that investigation is located overseas and was identified as not being related to the victim. Accordingly, your affiant believes **blairalex32** to be overstating his access to this minor victim for unknown

reasons.

13. The undercover continued to engage **blairalex32** in conversation. The undercover asked if **blairalex32** had any other material. **blairalex32** said he possessed additional material, including images of his purported student and more than 200 images of “a sophomore.” The undercover understood **blairalex32** to mean he has a collection of images and videos of other minors that is sexually exploitive. Based on the conversations with **blairalex32**, your affiant believes that **blairalex32** has collected the sexually exploitive material over an extended time period before the undercover engaged **blairalex32** in the chat.

14. Based on my professional experience, individuals who engage in the transportation, possession, receipt, and distribution of child pornography often store and maintain images, records, and communications relating to this illegal activity and often keep communications with other like-minded individuals saved in accounts. Because **blairalex32** engaged in a public online platform related to discussion of the sexual exploitation of children and, on such a platform, expressed his willingness to sell and distribute already possessed child pornography, and did complete such a transaction (meaning the Target sent to the OCE a link to download and view child pornography in exchange for money), your affiant has reason to believe that records relating to this illegal activity and to other persons involved with this activity will be saved in Target’s Subject Accounts. Through his conversation and interaction with the OCE, the Target exhibited that he is a person with a sexual interest in children and an interest in images of children engaged in sexually exploitive acts. The Target holds himself out as an individual who has access to the children whose sexually exploitive photos he is offering for sale. The Target purports to have a voluminous collection of such material, including a particular minor during a time range when the minor was 12 and 13 years old, and his

sale of child pornography to the OCE confirms possession of such exploitive material. Accordingly, your affiant has reason to believe that material depicting the sexual exploitation of minors is currently contained in the Subject Accounts. Additionally, based on your affiants training and experience, individuals who share child pornography rarely destroy correspondence from other distributors/collectors and may conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Therefore, your Affiant submits that information related to the Target's illegal activity will be contained in the Subject Accounts, including logs of online chats and contact information of co-conspirators, including telephone numbers, email addresses, IP logs and identifiers for instant messaging and social medial accounts.

15. Based on the foregoing, your affiant respectfully submits there is probable cause to believe that **blairalex32** is engaged in the creation, transportation, possession, receipt, and distribution of child pornography (the "Subject Offenses") and that **blairalex32** has communicated with other persons about the same. Therefore, your affiant submits that evidence of this criminal activity, as well as evidence of **blairalex32**'s identity and location, is likely to be found in the Google account associated with the Gmail email address **grantkeppel@gmail.com** and **blairalex32**'s Kik account (the "Subject Accounts").

16. Based upon the foregoing, I respectfully submit there is probable cause to believe that information created and stored on the Subject Accounts' provider's servers—from the date of the creation of the accounts through the present, and associated with the Subject Accounts, will contain evidence, fruits, contraband, and instrumentalities of the creation, transportation, possession, receipt,

and distribution of child pornography.

17. In particular, I believe the Subject Accounts are likely to contain the following information:

a. Evidence of the Subject Offenses, such as text communications, videos, images, and other stored content and information presently contained in, or on behalf of, the Subject Accounts that depict preparation for, and participation in, the Subject Offenses;

b. Evidence of communications between the Subject Accounts user(s), and potential co-conspirators related to the Subject Offenses, including identities and locations of co-conspirators;

c. The identities of victims of the Subject Offenses;

d. Evidence of the relationships between and among co-conspirators involved in the Subject Offenses;

e. Transactional information of all activity of the Subject Account, including log files, dates, times, methods of connecting, polls, dial-ups, and/or locations;

f. Subscriber information, in any form kept, pertaining to the Subject Account, including, but not limited to, applications, subscribers' full names, all display names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, detailed billing records, and associated device information and identifiers (e.g., IMEI number);

g. Evidence concerning the location of other evidence of the Subject Offenses, including but not limited to information concerning email or other social media accounts potentially containing relevant evidence;



h. Passwords or other information needed to access a user's electronic device(s) or other online accounts that may contain evidence of the Subject Offenses; and

i. Information related to other digital facilities which the user(s) of the Subject Account used or used, including but not limited to other Internet profiles, email addresses, and other social media platforms.

### **BACKGROUND CONCERNING THE PROVIDERS' ACCOUNTS**

18. **Google, LLC** is the provider of the internet-based account associated with the email address **grantkeppel@gmail.com**; **MediaLab.AI** is the provider of the chat application **Kik** which controls and maintains the Kik account associated with the username "**blairalex32**".

20. Based on my training, experience, and knowledge, I have learned the following about **Google, LLC**:

a. Google, LLC has used the slogan, "One account. All of Google." Based on my training and experience, I know that when a user opens a Google account, Google automatically assigns the user a Gmail email account by adding @gmail.com to the end of the user's self-appointed username. As such, if a user opened a Google account under the user name GovernmentUser1, the Google account would be created as GovernmentUser1@gmail.com. Under this system, Google has created a single sign-on access across all Google applications. Once the user opens a Google account, they have access to all Google services including: Gmail; Google Photos; Google+; YouTube; Blogger; Google Drive; Google Groups; Chrome Browser History; Google Docs; Calendar; Google Sites; and more.

b. Google, LLC provides a variety of services to the public, including free online storage space. Google, LLC's online storage service is known as "Google Drive," and is a file storage and synchronization service. Google Drive allows users to store files remotely on Google servers, synchronize files across devices, and share files. It is available on the Internet and as a mobile application. Files and folders stored in Google Drive can be shared privately with other users having a Google services account.

c. Google Photos is a photo sharing and storage service developed by Google and is available both on the Internet via website and as a mobile application. Google Photos gives users free unlimited storage space for photos and videos, under certain conditions, described below. Google Photos can be configured to automatically sync photos and videos taken with a user's camera to a user's Google Photo account. Like Google Drive, Google Photos allows users to store files remotely on Google servers, synchronize files across devices, and share files.

d. Google Drive and Google Photos are complementary parts of the same Google services account. Photos and videos are stored on a user's Google account's storage space with each account having 15 gigabytes (GB) of free storage, with the option to purchase additional storage space. Files uploaded to a user's Google account via Google Drive count against the 15 GB quota. Files uploaded via Google Photos do not count against the account's quota as long as they are uploaded as "High Quality" (Google's term). Google advertises that images/videos uploaded as "High Quality" get an unlimited amount of storage space. Images/videos uploaded in "Original Quality" (Google's term) do count against the account's quota. The difference between "High Quality" and "Original Quality" has to do with the amount of compression applied to a file, which affects the file's size.

e. The Google Photos mobile application is configured to automatically transfer and store graphics files created on the mobile device to the Google Photos service associated with the Google account. Users also have the option to manually transfer files between Google Photos and Google Drive.

f. Google, LLC allows subscribers to obtain Google Drive storage space at the domain name “gmail.com.” Subscribers obtain an account by registering with Google, LLC. During the registration process, Google, LLC asks subscribers to provide basic personal information. Therefore, the computers of Google, LLC are likely to contain stored information concerning subscribers and their use of Google, LLC services, such as account access information and account application information.

g. In general, files that are transferred to a Google Drive or Google Photos account are stored in the subscriber’s storage space on Google, LLC servers until the subscriber deletes the data. If the subscriber does not delete files, they can remain on Google, LLC servers indefinitely. Even if the subscriber deletes files, they may continue to be available on Google, LLC’s servers for a certain period of time.

h. A Google, LLC subscriber can also store files in addition to graphics, such as address books, contact or buddy lists, calendar data, and other files on servers maintained and/or owned by Google, LLC via the Google Drive service.

i. Google, LLC typically retains certain transactional information about the creation and use of each account on their system. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or

closed), and other log files that reflect usage of the account. In addition, Google, LLC logs and retains the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account.

21. Based on my training, experience, and knowledge, I have learned the following about **MediaLab.AI** and **Kik**:

a. Kik Messenger (hereinafter “Kik”) is a mobile application designed for chatting or messaging owned and operated by **MediaLab.AI**. According to the publicly available document “Kik’s Guide for Law Enforcement,”<sup>1</sup> to use the **Kik** application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

b. According to “Kik’s Guide for Law Enforcement,” Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily

---

<sup>1</sup> Available at:  
[https://www.kik.com/uploads/files/LEO1%201%20Kik\\_s%20Guide%20for%20Law%20Enforcement\\_September%202016.pdf](https://www.kik.com/uploads/files/LEO1%201%20Kik_s%20Guide%20for%20Law%20Enforcement_September%202016.pdf)

identifiable or searchable by keyword.

c. Kik may retain, at a minimum, the following user data:

1. Transmission data (including content) associated with messages sent or received by a user, the content of the message, and whether the message was deleted;
2. Media files, including data and information directly associated with, embedded in or attached to any image, video, audio, or text file associated with any transmissions sent from or received by a user during a specified time period; and
3. Logs of internet protocol ("IP") addresses.

d. The Provider may maintain preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). The Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

22. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require **Google, LLC** and **MediaLab.AI** to disclose to the government copies of the items information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

23. Based on the foregoing, I request that the Court issue the proposed search warrant.

24. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

25. The government will execute this warrant by serving the warrant on **Google, LLC** and **Kik (MediaLab.AI)**. Because the warrant will be served on Google, LLC and Kik (MediaLab.AI), who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

26. The above information is true and correct to the best of my knowledge, information and belief.

**REQUEST FOR SEALING**

24. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant and the requisite inventory notice (with the exception of one copy of the warrant and inventory notice that will be sent to Google, LLC and Kik (MediaLab.AI)). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on the continuing investigation and may otherwise jeopardize its effectiveness.

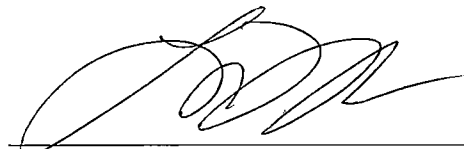
Respectfully submitted,



---

Matthew Patcher  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on February 28<sup>th</sup>, 2020



---

LISA PUPO LENIHAN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property/Location to Be Searched**

The property/location to be searched is the **Google, LLC** account identified by and/or associated with the email account/address, **grantkeppel@gmail.com**, and which is stored and maintained at premises owned, maintained, controlled, or operated by **Google, LLC**, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.



**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, LLC:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, LLC, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **Google, LLC**, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **Google, LLC** is required to disclose the following information to the government for the account or identifier listed in Attachment A:

- (a) All contact and personal identifying information about the subscriber of the Target Account, including names (subscriber names, user names, screen names, vanity names), user identification number, birth date, contact e-mail addresses, passwords, security questions and answers, physical address (including city, state, and zip code), and telephone numbers;
- (b) All documents, photos, images, and videos, including Exchangeable Image File (“EXIF”) data and any other metadata, along with the files’ storage structure and transaction information (i.e. logs detailing upload, deletion, sharing, etc.);
- (c) The contents of all emails and instant message communications associated with the Account, including stored or preserved copies of emails sent to and from the Account, draft and deleted emails/messages, the source and destination addresses associated with each email/message, the date and time at which each email/message was sent, and the size and length of each email/message;

- (d) All records or other information stored at any time by an individual using the Account, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logos, and files;
- (e) All records and other information concerning any computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;
- (f) All records or other information regarding the devices and/or Internet browsers associated with, or used in connection with, the Account, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (g) The identity of other accounts linked by machine cookie and the nature of the cookie (including where linked by machine cookie or other cookie, creation or login Internet protocol ("IP") address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise) ("Linked Accounts"); and, for each Linked Account, all records and information requested in Part I of this attachment;
- (h) All Accounts that are registered or subscribed using the Target Account (i.e., with any one of the Target Accounts in any subscriber information);

- (i) Any and all cookies associated with or used by any computer or web browser associated with the Target Account, including the IP addresses, dates, and times associated with the recognition of any such cookie.
- (j) All privacy settings;
- (k) All records pertaining to communications between Google LLC and any person regarding the user or the user's account, including contacts with support services and records of actions taken.
- (l) All records and other information relating to the Target Account, including:
  - 1. Records of user activity for each connection (including logins and logouts) made to or from the Target Account(s), including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; connectivity information to include account change history and password change history; full history of all logins to include cookie logins; raw AMT logs for account access; and source and destination Internet Protocol addresses;
  - 2. All IP logs and other documents showing the IP address, date, and time of each login and logout to the account, including "Active Sessions" information (all stored active sessions, including date, time, device, IP address, machine cookie and browser information);
  - 3. Information about each communication sent or received by the Target Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such

- as source and destination email addresses, IP addresses, and telephone numbers);
4. Accounts to which any Linked Accounts are themselves linked, other than the Target Accounts, by cookie, including machine cookie;
  5. Language settings information;
  6. All advertising data relating to the Target Account, including, but not limited to, information regarding unique advertising IDs associated with the Target Account, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), and Pixel information; and
  7. User agent information and device ID information, including all devices used to access the Target Account and Android IDs, including any information of any computers or cellphone devices utilized to access the account to include user agent strings, hardware cookies, IMEI numbers, device tokens, or push tokens.
- (m) All search history, web history, Google Web & App Activity or Google “History Events” by the user of above listed email address, including web clicks;
- (n) All web browsing activities that are identifiable with above listed email address or with machine cookies used to access above listed email address.
- (o) All records (including content records) pertaining to any Google service associated with above listed email addresses, including push tokens or services such as, but not limited to, Gmail, Google Maps, Google Calendar, Google Docs, Google Drive, Web History, and Hangouts;

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, contraband, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(1), 2252(a)(2), and 2252(a)(4)(B):

- (a) Records and information constituting, referencing, or revealing child pornography, as defined in 18 U.S.C. 2256(8);
- (b) Records and information constituting, referencing, or revealing child erotica;
- (c) Records and information constituting, referencing, or revealing the trafficking, advertising, creation or possession of child pornography, to include the identity of the individuals involved;
- (d) Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved;
- (e) Records and information constituting, referencing, or revealing communication or interaction of an illicit sexual nature with a minor, to include the identity of the individuals involved, including but not limited to, associated email accounts, accounts which share a cookie, login IP addresses, and session times and durations;
- (f) For all items described in this section above, all metadata, transaction information, storage structure, and other data revealing how the items were created, edited, deleted, viewed, or otherwise interacted with;
- (g) Records and information revealing or referencing information about the device(s) used to access the account;

- (h) Records and information revealing or referencing the identity of the individual who created and used the account; and
- (i) Identity of accounts linked by cookie, including machine cookie.

As used above, “child erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions. The term “minor” means any person under the age of 18 years.

### **III. Delivery of Information by Google, LLC to the Federal Government**

Within **14 days** of the issuance of this warrant, and notwithstanding Title 18, United States Code, Section 2252A or similar statute or code, Google, LLC shall disclose and deliver the information set forth above to the government via the United States Postal Service, another courier service, or email by sending to:

Special Agent Matthew Patcher  
Federal Bureau of Investigations  
3311 E Carson St  
Pittsburgh PA 15203  
mpatcher@fbi.gov  
646-831-2446

**ATTACHMENT A**

**Property/Location to Be Searched**

The property/location to be searched is the **Kik** account associated with the username “**bliralex32**” and which is stored and maintained at premises owned, maintained, controlled, or operated by **MediaLab.AI** (the “Provider”), a company headquartered in the United States at 1240 Morningside Way, Venice, CA 90291, and accepting service of legal process through email at lawenforcement@kik.com.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Kik (MediaLab.AI):**

To the extent that the information described in Attachment A is within the possession, custody, or control of **Kik (MediaLab.AI)**, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **Kik (MediaLab.AI)**, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **Kik (MediaLab.AI)** is required to disclose the following information to the government for the account or identifier listed in Attachment A, for the Account associated with the username “**blairalex32**”:

- (a) All contact and personal identifying information about the subscriber of the Target Account, including names (subscriber names, user names, screen names, vanity names), user identification number, birth date, contact e-mail addresses, passwords, security questions and answers, physical address (including city, state, and zip code), and telephone numbers;
- (b) All documents, photos, images, and videos, including Exchangeable Image File (“EXIF”) data and any other metadata, along with the files’ storage structure and transaction information (i.e. logs detailing upload, deletion, sharing, etc.);
- (c) The contents of all message communications associated with the Account, including stored or preserved copies of messages sent to and from the Account, draft and deleted messages, the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message;



- (d) All records or other information stored at any time by an individual using the Account, including address books, contact and buddy lists, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;
- (e) All records or other information regarding the devices and/or Internet browsers associated with, or used in connection with, the Account, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) The identity of other accounts linked by machine cookie and the nature of the cookie (including where linked by machine cookie or other cookie, creation or login Internet protocol ("IP") address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise) ("Linked Accounts"); and, for each Linked Account, all records and information requested in Part I of this attachment;
- (g) All Accounts that are registered or subscribed using the Target Account (i.e., with any one of the Target Accounts in any subscriber information);
- (h) Any and all cookies associated with or used by any computer or web browser associated with the Target Account, including the IP addresses, dates, and times associated with the recognition of any such cookie.
- (i) All privacy settings;
- (j) All records pertaining to communications between Kik (MediaLab.AI) and any person regarding the user or the user's account, including contacts with support services and records of actions taken.
- (k) All records and other information relating to the Target Account, including:

1. Records of user activity for each connection (including logins and logouts) made to or from the Target Account(s), including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; connectivity information to include account change history and password change history; full history of all logins to include cookie logins; raw AMT logs for account access; and source and destination Internet Protocol addresses;
2. All IP logs and other documents showing the IP address, date, and time of each login and logout to the account, including "Active Sessions" information (all stored active sessions, including date, time, device, IP address, machine cookie and browser information);
3. Information about each communication sent or received by the Target Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);
4. Accounts to which any Linked Accounts are themselves linked, other than the Target Accounts, by cookie, including machine cookie;
5. Language settings information;
6. All advertising data relating to the Target Account, including, but not limited to, information regarding unique advertising IDs associated with the Target Account, application IDs, UDIDs, payment information (including,

but not limited to, full credit card numbers and expiration dates and PayPal accounts), and Pixel information; and

7. User agent information and device ID information, including all devices used to access the Target Account(s) and Android IDs, including any information of any computers or cellphone devices utilized to access the account to include user agent strings, hardware cookies, IMEI numbers, device tokens, or push tokens.

- (l) All web browsing activities that are identifiable with above listed Target Account or with machine cookies used to access above listed Account.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, contraband, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(1), 2252(a)(2), and 2252(a)(4)(B) in the form of the following:

- (a) Records and information constituting, referencing, or revealing child pornography, as defined in 18 U.S.C. 2256(8);
- (b) Records and information constituting, referencing, or revealing child erotica;
- (c) Records and information constituting, referencing, or revealing the trafficking, advertising, creation or possession of child pornography, to include the identity of the individuals involved;
- (d) Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved;

- (e) Records and information constituting, referencing, or revealing communication or interaction of an illicit sexual nature with a minor, to include the identity of the individuals involved, including but not limited to, associated email accounts, accounts which share a cookie, login IP addresses, and session times and durations;
- (f) For all items described in this section above, all metadata, transaction information, storage structure, and other data revealing how the items were created, edited, deleted, viewed, or otherwise interacted with;
- (g) Records and information revealing or referencing information about the device(s) used to access the Account;
- (h) Records and information revealing or referencing the identity of the individual who created and used the Account, including any available geolocation information; and
- (i) Identity of accounts linked by cookie, including machine cookie.

As used above, “child erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions. The term “minor” means any person under the age of 18 years.

### **III. Delivery of Information by Kik (MediaLab.AI) to the Federal Government**

Within **14 days** of the issuance of this warrant, and notwithstanding Title 18, United States Code, Section 2252A or similar statute or code, **Kik (MediaLab.AI)** shall disclose and deliver the

information set forth above to the government via the United States Postal Service, another courier service, or email by sending to:

Special Agent Matthew Patcher  
Federal Bureau of Investigations  
3311 E Carson St  
Pittsburgh PA 15203  
mpatcher@fbi.gov  
646-831-2446